UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,200	12/31/2003	W. Dale Hopkins	200309348-1	9964

22879 7590 07/30/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
07/30/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/749,200
Filing Date: December 31, 2003
Appellant(s): HOPKINS ET AL.

Nathan E. Stacy
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5/24/2010 appealing from the Office action mailed 12/28/2009.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1-31

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

4747050	Brachtl	5-1988
1310719	Vernam	7-1919
4924514	Matyas	5-1990

IBM Research Report, Triple DES Cipher Block Chaining with Output Feedback Masking, D. Coppersmith, D.B> Johnson, S.M. Matyas, 10/21/1996

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-3, 7-10, 11-13, 16-21 and 24-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith.

Regarding Claims 1-2, 7 and 9

Matyas teaches a first input block that is a text block containing a secret PIN, a second input block derived from a non-secret entity identifier independent of the PIN , and a PIN verification Key.*(See Figure 10, also Column 22, especially "KPV is the 64-bit PIN validation key…PIN is a 64 bit input PIN in clear form…valid data is a 64 bit users data padding included")*

Matyas does not explicitly teach a plurality of cipher blocks linked in a Cipher Block Chain (CBC) and keyed with a Key;

a first input block coupled to a first cipher block in the CBC chain capable of receiving a text block.

and a second input block coupled to a second cipher block in the CBC chain capable of receiving a text block and ciphertext from a cipher block in the CBC chain.

a logical operator that exclusive-ORs the plaintext block derived from the secret PIN with an initialization vector to produce an initialized block

a first encryptor that encrypts the initialized block using 3-DES encryption to produce a first ciphertext block ;

a logical operator that exclusive-ORs the plaintext block derived from the with the first ciphertext block to produce a chained block;

and a second encryptor that encrypts the chained block using 3-DES encryption to produce a second ciphertext block

Coppersmith teaches an apparatus comprising:

a plurality of cipher blocks linked in a Cipher Block Chain (CBC) and keyed with a Key; *(Figure 1 shows Triple-DES external feedback cipher block chaining)*

a first input block *(Figure 1, X1)* coupled to a first cipher block *(Figure 1, Y1)* in the CBC chain capable of receiving a text block.

and a second input block *(Figure 1, X2)* coupled to a second cipher block *(Figure 1, Y2)* in the CBC chain capable of receiving a text block and ciphertext from a cipher block in the CBC chain.

a logical operator that exclusive-ORs the plaintext block derived from the secret PIN with an initialization vector to produce an initialized block *(Figure 1, the Examiner interprets IV as being the initialization vector, and X1 as the plaintext block. The Examiner interprets the XORed result of IV and X1 as the initialized block);*

a first encryptor that encrypts the initialized block using 3-DES encryption to produce a first ciphertext block ; *(Figure 1. The Examiner interprets the first encryptor as the Triple-DES encryptor between X1 and Y1)*

a logical operator that exclusive-ORs the plaintext block derived from the with the first ciphertext block to produce a chained block; *(Figure 1. The Examiner interprets the first ciphertext block as Y1 and the plaintext block as X2 and the XOR in between as the logical operator)*

and a second encryptor that encrypts the chained block using 3-DES encryption to produce a second ciphertext block *(Figure 1. The Examiner interprets the second encryptor as the Triple-DES encryptor between X2 and Y2)*

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Matyas to use the Triple DES encryption as taught by Coppersmith.

The claim would have been obvious because the substitution of one known element (Triple DES taught by Coppersmith for Block cipher of Matyas) would have yielded predictable results to one of ordinary skill in the art at the time of the invention. The substitution would be particularly obvious because Triple DES is a well known type of Block Ciphering.

Regarding Claim 3,

Matyas and Coppersmith teaches the apparatus according to claim 2 wherein: the PIN verification apparatus operates in a reversible mode that enables recovery of

the secret PIN from the second ciphertext block. *("the customer's PIN is recovered from the decrypted PIN block" Column 4)*

Claim 4-5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith further in view of Vernam (1310719).

Regarding Claims 4 and 5,

Matyas and Coppersmith teach the apparatus according to claim 2. However they do not explicitly teach further comprising: a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block.

Vernam teaches a cipher that takes in two inputs and XORs them together to produce a ciphertext. The Vernam cipher has been a well known way to provide further encryption since 1919.

It would have been obvious to one of ordinary skill in the art at the time of the invention to XOR together the first and second ciphertext block to produce a third ciphertext block.

The motivation is to provide further encryption.

It is inherent that a PIN verification apparatus operates in an irreversible mode when the secret key is not possessed.

Regarding Claim 8,

Matyas and Coppersmith teach the apparatus according to Claim 1.

Matyas teaches a format converter capable of converting hexadecimal digit ciphertext to decimal result by scanning the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits. (Figure 9 shows a hexadecimal ciphertext input into a decimalization table. The Examiner interprets the output digits as the PIN Verification Value. The Examiner further interprets that it is inherent that a predetermined number of digits must first be selected before converting from hex to decimal.

Regarding Claim 10,

Matyas and Coppersmith teaches the apparatus according to claim I.

Matyas teaches a length digit *("a-pin-len is the number (1-16) indicating how many digits the generated PIN is assigned to the customer" Column 20, lines 53-53,* x hexadecimal digits of the secret PIN *("CPIN is a…customer selected PIN in clear form" Column 20, lines 41-47)*, a non-secret identifier and a pad character for the non-secret identifier that is repeated 16- (number of digits in the non-secret identifier) times *("val-data, Validation data is a 64-bit plain user's data, padding included. Ordinarily it will be the user's PAN" Column 20, lines 51-53)*.

Coppersmith and Mayas do not explicitly teach a first formatter configured to construct a first incoming plaintext block from a concatenation of a length digit x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier;

and a second formatter configured to construct a second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

It would have been obvious to one of ordinary skill in the art at the time of the invention to construct a first plaintext block by concatenating a length digit with x hexadecimal digits of a PIN and 16-(x+1) hexadecimal digits of a non-secret entity identifier, and to construct a second plaintext block by concatenating y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

The motivation to construct the first plaintext block by concatenating a length digit with a PIN and 16-(x+1) digits is firstly because it is a plaintext block and the user can choose to input the block in any suitable format. The IBM 3624 format already includes the length digit, the PIN as well as a pad for the PIN that is 16-x in length. It would have been very obvious to one of ordinary skill to modify the IBM 3624 format to include these three inputs in a first format.

The motivation to construct the second plaintext block by concatenating y hexadecimal digits of the non-secret entity identifier with a pad character that is repeated 16-y times is that the non-secret entity identifier (val-data) already comes padded in the IBM 3624 format. Without any modification the user could, as their design choice, input the val-data into the second plaintext block as described in Coppersmith. The concatenation of elements already taught by the prior art (length digit, hex digit, non-secret entity, etc.) would yield predictable results to one of ordinary skill in the art.

Regarding Claims 11-13, 18, 20-21, 28-31

Matyas teaches a data security apparatus comprising:

an enrollment terminal capable of accepting a magnetic stripe card storing a non-secret entity-identifier and an entity-selected secret Personal Identification Number (PIN); *(Figure 3, EFT Terminal accepts a PIN and is capable of storing non secret entity identifier)*

a processor coupled to the enrollment terminal and capable of receiving the entity-identifier and the PIN; *(It is inherent that the EFT Terminal has a processor capable of receiving the entity-identifier)*

and a memory coupled to the processor *(It is inherent that the EFT Terminal has memory with code embodied on it)* and having a computable readable program code embodied therein capable of causing the processor to enroll a PIN *(Figure 3. Create PIN block)*:

a database capable of storing a plurality of PIN Verification Values (PVVs) for enrolled magnetic stripe cards; *(Figure 3, Customer Accounts Database).*

an escrow capable of storing a plurality of escrow values associated with at least some of the enrolled magnetic stripe cards; *(Figure 3, Institution Y is capable of storing escrow values)*

and a processor coupled to the database and the escrow and capable of receiving an entity-identifier, a PIN Verification Value (PVV) associated to the entity-identifier, and at least one escrow value associated to the entity-identifier; *(Figure 3, HPC, or the Host Processing Center inherently has a processor that is capable or receiving identifiers and values)*

and a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to recover a PIN. *(Figure 3, The HPC and Institution Y inherently have memories capable of causing the processor to recover a PIN as shown by the Verify PIN function)*

a plurality of terminals coupled to the servers via the network *(Figure 1, EFT Terminals);*

a plurality of magnetic stripe cards enrolled in the transaction system and capable of insertion into the on-line terminals and performing transactions via the servers; *("Consider the network configuration as shown in Fig 1. The entry point at which*

transaction requests are intiated, such as a point of sale (POS) terminal or an automated teller machine (ATM), is defined as an EFT terminal." Column 2, lines 46-49). It is inherent that an ATM includes a plurality of magnetic stripe cards enrolled in the transaction system and capable of insertion into the online terminals and performing transactions via the servers.

and a plurality of processors distributed among the servers, hosts, and/or the terminals, at least one of the processors being capable of executing PIN verification using a magnetic stripe card. *(Figure 1, the Host Processing center and the terminals inherently have processors, of which the processors are capable of executing PIN verification)*

means for writing the PVV to a transaction card for subsequent PIN verification *(Figure 5, shows the Remote Card Issuing Station writing PIN information to a transaction card via the Card Writer)*

Matyas teaches a first input block that is a text block containing a secret PIN, a second input block derived from a non-secret entity identifier, and a PIN verification Key.*(See Figure 10, also Column 22, especially "KPV is the 64-bit PIN validation key…PIN is a 64 bit input PIN in clear form…valid data is a 64 bit users data padding included")*

Matyas does not teach a method of linking a plurality of cipher blocks, applying incoming plaintext blocks to cipher blocks, keying the cipher blocks with a key, XORing the plaintext block with an initialization vector, encrypting the initialized block using tripled DES encryptiong, XORing the plaintext block with the first ciphertext block, encrypting the chained block using triple DES encryption, and outputting the second cipher block.

Coppersmith teaches a method comprising:

linking a plurality of cipher blocks in a Cipher Block Chain (CBC); *(Figure 1 shows Triple-DES external feedback cipher block chaining)*

applying an incoming plaintext block to one of the plurality of cipher blocks; *(Figure 1 shows applying the plaintext block (X1) to a cipher block (Y1))*

applying an incoming plaintext block derived from a non-secret entity-identifier and ciphertext from a cipher block in the CBC chain; *(Figure 1 shows applying the plaintext block (X2) to a cipher block (Y2)) The Examiner interprets the X1 as the non-secret entity identifier and Y2 as the cipher block.*

keying the plurality of cipher blocks with a Key; and executing the cipher blocks resulting in generation of ciphertext (Figure 1. shows the plaintext being keyed (K1-K3) resulting in the generation of ciphertext.

exclusive-ORing the plaintext block with an initialization vector to produce an initialized block; *(Figure 1, the Examiner interprets IV as being the initialization vector, and X1 as the plaintext block. The Examiner interprets the XORed result of IV and X1 as the initialized block);*

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block; *(Figure 1. The Examiner interprets the first encryptor as the Triple-DES encryptor between X1 and Y1)*

exclusive-ORing the plaintext block with the first ciphertext block to produce a chained block; *(Figure 1. The Examiner interprets the first ciphertext block as Y1 and the plaintext block as X2 and the XOR in between as the logical operator)*

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; *(Figure 1. The Examiner interprets the second encryptor as the Triple-DES encryptor between X2 and Y2)*

and outputting the second ciphertext block (*The Examiner interprets the output of the second ciphertext block as supplying information)*

It is inherent that with the proper key information the original cleartext can be recovered.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the processor of Matyas perform the method of Coppersmith.

The motivation is that the method of using a CBC using triple-DES encryption is well known in the art. One of ordinary skill would be able to use the method of Coppersmith on the terminal of Matyas for the purpose of PIN encryption.

Coppersmith however does not teach that the first input block that is a text block contains a secret PIN. Coppersmith further does not teach that the second input block is derived from a non-secret entity-identifier. Coppersmith does not teach that the key is a Pin Verification Key. Coppersmith does not teach that the output of the second ciphertext block is to be used for the purpose of PIN verification.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the system of Coppersmith input a secret PIN in the first input block and input a non-secret identifier in the second input block and have the key be a PIN verification key.

The motivation is that the system of Coppersmith without any modification can take the inputs of a secret PIN and the non-secret identifier and using a key output a Pin Verification Value. Furthermore CBC can generate ciphertext for any field. One of ordinary skill in the art would be able to take the ciphertext generated from the inputs for the purpose of PIN verification.

Regarding Claims 16 and 24,

Matyas and Coppersmith teach the method according to claim 11 and the security apparatus that invokes the method in claim 20.

Matyas teaches a format converter capable of converting hexadecimal digit ciphertext to decimal result by scanning the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits. (Figure 9 shows a hexadecimal ciphertext input into a decimalization table. The Examiner interprets the output digits as the PIN Verification Value. The Examiner further interprets that it is

inherent that a predetermined number of digits must first be selected before converting from hex to decimal.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the PIN verification apparatus of Coppersmith with the format converter of Matyas.

The motivation is that Figure 9 describes the IBM 3624, including the format converter. This PIN verification apparatus is very well known in the PIN verification art and has been in use since the late 1970's. Therefore one of ordinary skill in the art would know to add a hexadecimal to decimal format converter to a PIN verification apparatus and the results would be predictable.

Regarding Claims 17 and 25,

Matyas and Coppersmith teach the method according to claim 11 and the security apparatus that invokes the method in claim 20. Matyas and Coppersmith do not explicitly teach supplying hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) as a PIN Verification Value (PVV).

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the final ciphertext be in hexadecimal format.

The claim would have been obvious because the substitution of one known format for another (hexadecimal) would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Regarding Claims 19 and 27,

Matyas and Coppersmith teaches the method according to claim 11 and the security apparatus that invokes the method in claim 20.

Matyas teaches a length digit *("a-pin-len is the number (1-16) indicating how many digits the generated PIN is assigned to the customer" Column 20, lines 53-53,* x hexadecimal digits of the secret PIN *("CPIN is a…customer selected PIN in clear form" Column 20, lines 41-47)*, a non-secret identifier and a pad character for the non-secret identifier that is repeated 16- (number of digits in the non-secret identifier) times *("val-data, Validation data is a 64-bit plain user's data, padding included. Ordinarily it will be the user's PAN" Column 20, lines 51-53)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the apparatus of Coppersmith with the inputs of Mayas.

The motivation to combine is that Mayas discloses the inputs of the Generate IBM 3624 PIN process. This PIN verification apparatus is very well known in the PIN verification art and has been in use since the late 1970's. Therefore one of ordinary skill in the art would know of these inputs.

Coppersmith and Matyas do not explicitly teach a first formatter configured to construct a first incoming plaintext block from a concatenation of a length digit x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier;

and a second formatter configured to construct a second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

It would have been obvious to one of ordinary skill in the art at the time of the invention to construct a first plaintext block by concatenating a length digit with x hexadecimal digits of a PIN and 16-(x+1) hexadecimal digits of a non-secret entity identifier, and to construct a second plaintext block by concatenating y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

The motivation to construct the first plaintext block by concatenating a length digit with a PIN and 16-(x+1) digits is firstly because it is a plaintext block and the user can choose to input the block in any suitable format. The IBM 3624 format already includes the length digit, the PIN as well as a pad for the PIN that is 16-x in length. It would have been very obvious to one of ordinary skill to modify the IBM 3624 format to include these three inputs in a first format.

The motivation to construct the second plaintext block by concatenating y hexadecimal digits of the non-secret entity identifier with a pad character that is

repeated 16-y times is that the non-secret entity identifier (val-data) already comes padded in the IBM 3624 format. Without any modification the user could, as their design choice, input the val-data into the second plaintext block as described in Coppersmith.

The concatenation of elements already taught by the prior art (length digit, hex digit, non-secret entity, etc.) would yield predictable results to one of ordinary skill in the art.

Claims 14 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith as applied to claims 11 and 20 above, and further in view of Vernam.

Regarding Claims 14 and 22,

Matyas and Coppersmith teach the method according to claim 11 and the security apparatus that invokes the method in claim 20 wherein the PIN verification method is capable of operating in an irreversible mode that obstructs recovery of the secret PIN, the method comprising:

exclusive-ORing the plaintext block with an initialization vector to produce an initialized block; *(Figure 1 of Coppersmith, the Examiner interprets IV as being the initialization vector, and X1 as the plaintext block. The Examiner interprets the XORed result of IV and X1 as the initialized block);*

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block; *(Figure 1 of Coppersmith. The Examiner interprets the first encryptor as the Triple-DES encryptor between X1 and Y1)*

exclusive-ORing the plaintext block with the first ciphertext block to produce a chained block; *(Figure 1 of Coppersmith. The Examiner interprets the first ciphertext block as Y1 and the plaintext block as X2 and the XOR in between as the logical operator)*

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; *(Figure 1 of Coppersmith. The Examiner interprets the second encryptor as the Triple-DES encryptor between X2 and Y2)*

and outputting the second ciphertext block (*The Examiner interprets the output of the second ciphertext block as supplying information)*

Coppersmith does not exclusively teach exclusive-ORing the first ciphertext block with the second ciphertext block to produce a third ciphertext block;

Vernam teaches a cipher that takes in two inputs and XORs them together to produce a ciphertext.

It would have been obvious to one of ordinary skill in the art at the time of the invention to XOR together the first and second ciphertext block to produce a third ciphertext block.

The motivation is to provide further encryption.

It is inherent that a PIN verification apparatus operates in an irreversible mode when the secret key is not possessed.

Claims 6, 15, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith in view of Vernam, and further in view of Brachtl.

Regarding Claim 6,

Matyas Coppersmith and Vernam teach the apparatus according to claim 5. Coppersmith and Vernam do not further teach: an escrow storage coupled to the second encryptor and capable of storing the second ciphertext block.

Brachtl teaches an escrow storage coupled to a second encryptor capable of storing a second ciphertext block. *("The quantities AP KTR1 and KTR2 are stored at the*

issuer's data processing center enciphered under the second variant (KM2) of the issuer's master key and associated together and enclosed by the PAN for the user. The quantities PAN, PIN and KP for the user are also stored offline." Column 7, lines 49-56)

The Examiner interprets the escrow storage as the issuer's data processing center. The Examiner interprets the storage coupled to a second encryptor as the quantities being enciphered under the second variant. The Examiner further interprets that the second ciphertext block is capable of being stored.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Coppersmith and Vernam with an escrow storage.

The motivation is firstly "for backup purposes" Column 7, line 55. The second motivation is that the reference is a patent from 1988 so therefore it has been well known to store data in an escrow storage in the PIN verification art.

Regarding Claims 15 and 23,

Matyas, Coppersmith and Vernam teach the method and the security apparatus according to claim 14. The cited references do not further teach: storing the second ciphertext block in at least one escrow to facilitate recovery of the secret PIN.

Brachtl teaches an escrow storage coupled to a second encryptor capable of storing a second ciphertext block. *("The quantities AP KTR1 and KTR2 are stored at the issuer's data processing center enciphered under the second variant (KM2) of the issuer's*

master key and associated together and enclosed by the PAN for the user. The quantities PAN, PIN and KP for the user are also stored offline." Column 7, lines 49-56)

The Examiner interprets the escrow storage as the issuer's data processing center. The Examiner interprets the storage coupled to a second encryptor as the quantities being enciphered under the second variant. The Examiner further interprets that the second ciphertext block is capable of being stored.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Coppersmith and Vernam with an escrow storage.

The motivation is firstly "for backup purposes" Column 7, line 55. The second motivation is that the reference is a patent from 1988 so therefore it has been well known to store data in an escrow storage in the PIN verification art

(10) Response to Argument

A.

Appellant proposes that Matyas and Coppersmith do not teach "a second input text block that receives a second plaintext block derived from a non-secret entity-identifier that is *independent* of the PIN (pg. 12 of Appeals Brief)."

The Appellant further argues "In contrast, Matyas describes a technique where a first input to the cryptographic algorithm is the PIN, but the second input is an IBM 3624

formatted Pin that is derived from validation data and a PIN validation key (which is derived from the PIN and which is specifically contrary to the present claims (pg. 12)."

As previously argued by the Examiner's Final Office Action (pg. 2 Response to Arguments), "The Natural PIN (the Intermediate PIN of Matyas) is the PAN (Personal Account Number) encrypted with the PGK (PIN Generating Key). As the natural PIN is distinct from the customer selected PIN, the cited second input is already independent of the PIN."

The Applicant argues "However, the Matyas technique utilizes a PIN validation key, which is derived from the PIN. Moreover, the characterization of the Matyas intermediate PIN as a natural PIN supports the Appellant's argument that the Matyas intermediate PIN is not independent of the secret PIN (Appeal Brief pg. 13)."

The Examiner disagrees. The intermediate PIN is a temporary password. The customer *selected* PIN is *independently* chosen from the intermediate PIN. More succinctly, the customer selected PIN is not derived from the intermediate PIN. Because the customer selected PIN is selected in whichever way the customer wishes and the intermediate PIN is generated from a set PAN number plus a PIN generating key, the Examiner does not agree that the customer selected PIN is generated in a way that is dependent upon the intermediate PIN.

B.

Appellants argues “Claim 4 recites ‘a logical operator that exclusive-Ors the first ciphertext block with the second ciphertext block to produce a third ciphertext block”… “Vernam does not teach first and second ciphertexts that are formed and combined to produce a ciphertext, but rather merely discloses a combination of a plaintext block with a ciphertext block. (pg. 15 of Remarks)”

The Examiner argued “Vernam teaches taking two inputs and using XOR to produce a cipher text. (pg. 15 of Appeal Brief).”

The Applicant argues “However, the references, whether taken alone or in combination, do not disclose "a logical operator that exclusive-ORs the first ciphertext block witht eh second ciphertext block to produce a third ciphertext block" as claimed.

Vernam in Column 5 describes an input A (lines 5-7) exclusive-ORed with an input B (lines 24-26) and the ciphertext that results (lines 59-61). This teaches teaching a “first and second ciphertexts that are formed and combined to produce a ciphertext,”

C.

Appellant argues “Claim 5 recites ‘wherein the PIN verification apparatus operates in an irreversible mode that obstructs recovery of the secret PIN. (pg. 15 of Appeal Brief).” Matyas teaches encrypting the secret PIN several times (Figure 10, “Decrypt if PIN is encrypted”) If the PIN is encrypted it obstructs recovery of the secret PIN.

D.

Appellant argues "Vernam does not remedy the deficiencies of Matyas and coppersmith, as discussed above. Therefore, claims 14 and 22 are patentable over the instance combination because of their dependency." This argument is unpersuasive for the same rationale as the claims they are dependent upon.

E.

Appellant argues "Claim 15 (and Claim 23) recites "storing the second ciphertext block in at least one escrow to facilitate recovery of the secret PIN…IN contrast, while Brachtl discloses the general concept of escrow storage the combined references do not teach storing a ciphertext block in escrow storage to *facilitate recovery of the secret PIN. (pg. 18 of the Appeal Brief)*"

At the outset, the limitation "to facilitate recovery of the secret PIN" can be considered intended use as it does not require the recovery of the PIN but only to facilitate recovery. Secondly, Brachtl does describe holding ciphertext in escrow. Page 22 of the Final Office Action reads "The Examiner interprets the storage coupled to a second encryptor as the quantities being enciphered under the second variant."

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Harris C Wang/

Examiner, Art Unit 2439

Conferees:

/Christian LaForgia/

Primary Examiner, Art Unit 2439

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439